網路系統與安全期中報告

A.9 APACHE NETBEANS: DEVELOPMENT PLATFORM

從文章中可以知道攻擊者是先上傳一個含有惡意軟件的方案供使用者使用，而這些惡意軟件也就會攻擊供應商的資產並感染供應商的方案，而這些被感染的方案會被上傳到 GitHub 平台上，再由其他供應商下載這些方案，以此來破壞整條供應鏈。

其中攻擊者所使用的惡意軟件:

The Octopus Scanner Malware: 這種類型的惡意軟件攻擊 GitHub 系統上的存儲庫。Octopus Scanner 感染發生在開發人員下載受感染的儲存庫並使用它來創建軟件程序後。

Octopus Scanner 是一種後門惡意軟件，允許其創建者從受感染用戶那裡獲取信息。由於主要受感染用戶是開發人員，因此獲得的訪問權限對攻擊者來說非常重要，因為開發人員通常可以訪問其他項目、生產環境、數據庫密碼和其他關鍵資產。訪問權限升級的潛力巨大，在大多數情況下，這是攻擊者的核心目標。

Octopus Scanner 在開發人員從 GitHub 下載受感染的項目並基於它構建軟件後被激活。一旦激活，Octopus Scanner 就會掃描受感染的計算機，目的是找出其上是否安裝了 NetBeans IDE。NetBeans IDE 是一個基於 Java 的集成開發環境。

如果目標計算機不包含 NetBeans IDE，Octopus Scanner 將不會採取任何進一步行動。但是，如果 Octopus Scanner 檢測到 NetBeans IDE，它會用一個 dropper 感染構建文件。術語“dropper”是指一種旨在安裝其他惡意軟件的惡意軟件。在 Octopus Scanner 的情況下，dropper 會安裝遠程訪問木馬 (RAT)。

RAT 允許攻擊者控制受感染的機器。Octopus Scanner 的另一個重要特點是它不允許用新項目替換受感染的項目，從而確保惡意軟件不會被刪除。此外，Octopus Scanner 不僅會感染構建的文件，還會感染受感染項目的源代碼。

GitHub 發現 Octopus Scanner 很難被反惡意軟件應用程序檢測到。Octopus Scanner 尤其難以被 GitHub 刪除，因為擁有儲存庫的開發人員不知道感染情況，因此正在使用它們來開發合法軟件。因此，如果 GitHub 關閉儲存庫並刪除帳戶，公司將對各種合法軟件應用程序的開發產生負面影響。

防範方式:

一種防止 Octopus Scanner 的簡單方法是**不使用 NetBeans**。因為它不是最常用的 Java IDE。其他方法包括使用 GitHub 依賴關係圖、**自動安全更新**、**代碼掃描**和針對易受攻擊的依賴項的安全警報。